UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

LAW FIRM OF OMAR T. MOHAMMEDI, LLC,

Plaintiff,

– against –

COMPUTER ASSISTED PRACTICE ELECTRONIC MANAGEMENT SOLUTIONS, *d/b/a CAPEMS, Inc.*, KENNETH CULLEN, *individually and in his professional capacity*, JUSTIN GORKIC, *individually and in his professional capacity*,

Defendants.

OPINION AND ORDER

17 Civ. 04567 (ER)

RAMOS, D.J.:

The Law Firm of Omar T. Mohammedi, LLC, (the "Law Firm") brings this action against its former information technology provider, Computer Assisted Practice Electronic Management Solutions ("CAPEMS"), and its owners, Kenneth Cullen and Justin Gorkic, for violations of the Computer Fraud and Abuse Act ("CFAA") and New York state common law. Defendants move for summary judgment on all claims. For the reasons set forth below, the motion is GRANTED as to the federal claim and the state claims are DISMISSED for lack of jurisdiction.

I. Background

On December 16, 2011, the Law Firm entered into a contract with CAPEMS pursuant to which CAPEMS agreed to install a new server, to configure workstations for that server, to create a secure corporate email domain accessible by that server, and to provide maintenance for the system. Doc. 102-3, 2.[1] The contract also provided that CAPEMS "will configure [the Law

[1] The contract was a month-to-month agreement. Doc. 96-7, 3.

Firm's] remote backup service to provide an encrypted, offline backup." *Id.* at 3. As required by the contract, CAPEMS installed applications on the Law Firm's computers to send information automatically to CAPEMS's servers to back up the Law Firm's information remotely. Doc. 102-15, 27–30.

For many reasons unrelated to the motion at issue—including a Law Firm hard drive purportedly lost and a tablet computer rendered inoperable by CAPEMS—the relationship between CAPEMS and the Law Firm deteriorated. On December 28, 2016, Cullen wrote Omar Mohammedi, the Law Firm's managing partner, "[y]our next invoice has been voided," "any payment received will be returned," and "no further work will be performed by CAPEMS." Doc. 102-14, 12–13. Later that day, Mohammedi responded, "I am just as happy to find another reputable and professional company to take over," and "I would like to remind you about your obligation to keep everything intact until then." Doc. 102-14, 12.

Around this time, Mohammedi contacted Syed Mumtaz of Safe Haven and Complete Solutions ("Complete Solutions, Inc./Safe Haven Computers") to provide the information technology services that CAPEMS previously provided. Doc. 104, 3. As part of this transition, Mohammedi wrote Cullen to request the username and password for the server, telling him that "I am being held hostage as you have all that information." Doc. 102-14, 11–12. He further explained that this was "a major liability" because he wanted Mumtaz's firms to take over and complete certain tasks before January. *Id.* at 3.

Later that day Cullen responded that Mohammedi was mistaken, that they had already provided him with an administrative account, and that "any competent tech" could reset the password. Doc. 102-14, 11.

On January 1, 2017, Mohammedi gave Mumtaz the contact information for CAPEMS. Doc. 102-15, 32. In a series of emails over the next approximately two weeks, Mumtaz requested a variety of information concerning the Law Firm's computer system, including about passwords for various applications and workstations.

As relevant to the instant motion, on January 2, 2017, Mumtaz emailed Gorkic for more information about Crashplan, the offsite program that backed up the Law Firm's data and placed it in cloud storage owned by CAPEMS. Doc. 102-15, 30. Mumtaz asked if the Law Firm could continue to use the Crashplan software and store the data on CAPEMS's cloud. Gorkic explained that "we are no longer providing that service" to the Law Firm and that it "will have to find an alternative." *Id.*

In an email sent on January 6, 2017, Gorkic explained to Mumtaz, among other things, that "[w]e're also seeing data still coming from his network" and that the Law Firm "probably should uninstall remaining items we had installed related to monitoring etc." *Id.* at 27–28. There appears to be no dispute that the Law Firm did not remove the applications from its computers. Cullen and Mumtaz testified that, even after the termination of the contract, CAPEMS continued to receive and save information from the Law Firm. Cullen testified that CAPEMS, at the direction of its attorney, transferred the Law Firm's data from a server to an external storage device. Doc. 102-7, 15.[2] Mumtaz affirmed that CAPEMS "accessed the server without authority," "copied Plaintiff's client data," and created an external hard drive that contained Plaintiff's data. Doc. 104, 6.[3]

---

[2] In his deposition Gorkic testified that between the termination of the contract with the Law Firm and the date he delivered the backup data to his counsel in the summer of 2017, he never accessed or opened any of the files belonging the Law Firm. Doc. 102-12, 24. He further testified that he never reviewed or modified the files. Doc. 102-12, 24–25.

[3] In his affidavit, Mumtaz affirms, "At a time when Safe Haven had access to Plaintiff's server and were attempting to change passwords, it came to the attention of Safe Haven that Defendants, over the course of a weekend, had

Gorkic testified that he did not remove these applications himself because he "didn't want to touch the backup system as much as possible," "because [he] knew [Mohammedi] was going to sue [him]," and because he "didn't want [Mohammedi] to claim [he] modified the data." Doc. 102-12, 14–15.

On January 9, 2017, a Safe Haven technician spent three hours addressing problems with the Law Firm's wireless internet. Doc. 102-30, 2. The next day, January 10, that technician spent one and a half hours resolving issues with the Law Firm's email server. *Id.* at 3. Nine days later, January 19, another technician spent an hour resolving issues with the Law Firm's website. *Id.* On January 26, another technician spent forty-five minutes connecting a Law Firm employee's computer to the internet. *Id.* at 4. On January 30, another technician spent forty-five minutes connecting a Law Firm employee's computer to the printer. *Id.* In February 2017, Safe Haven sent the Law Firm an invoice for $1,058.06 for the work performed by its technicians. Doc. 102-30, 2–5.

Pursuant to Mohammedi's request, Mumtaz prepared a Network Report on February 14, 2017. Doc. 102-17, 2–3. According to the report, he recommended in part that the Law Firm replace the old firewall because the original was attached to CAPEMS's email. *Id.* at 3. He also reported that "there is currently no backup." *Id.* Mumtaz subsequently created onsite and offsite backup "from scratch." Doc. 102-10, 7.

In a letter to Cullen and Gorkic, dated February 24, 2017, Mohammedi asked that they return all data stored offsite or certify in writing that they had destroyed all data within their possession by March 6, 2017. Doc. 102-18, 2. The letter also asked Cullen and Gorkic to pay

---

attempted to access Plaintiff's server over sixty (60) times" and that "Defendants breached Plaintiff's server by attempting to log in." Doc. 104, 5.

$400 for the service they allegedly failed to provide in December and $1,058.06 for the service that Safe Haven provided. *Id.* at 2–3. The letter threatened that, "[o]therwise we will proceed with a legal action against you to seek substantial remedies." *Id.* at 3.

In a letter to Mohammedi, dated March 17, 2017, a lawyer for Cullen and Gorkic said that his clients would not pay the requested sum. Doc. 102-19, 2. He further explained that he had advised his clients to copy all of the Law Firm's information from their cloud, to create two copies of the data, one for the Law Firm and one to be held in escrow, and to destroy the rest. Doc. 102-19, 2–3. The letter indicated that the lawyer had told his clients to create a copy for escrow as evidence of the work provided to the Law Firm. *Id.* According to the letter, the lawyer would destroy the extra copy if the Law Firm decided not to sue. *Id.*

On June 16, 2017, the Law Firm filed the instant suit. Doc. 1. The suit claimed violations of CFAA, 18 U.S.C. § 1030, breach of contract, breach of covenant of good faith and fair dealing, conversion, trespass to chattel, unjust enrichment, and tortious interference with a contract and business relationship. *Id.*

On June 29, 2017, Plaintiff filed an amended complaint that mirrored the original complaint except that it claimed damages of "no less than $1,000,000." Doc. 12, 21, 29, and 31. Around the same time, Safe Haven sent the Law Firm an invoice for $2,828.99 to create onsite and offsite backup storage. Doc. 102-31, 2–3. However, it is unclear from the invoice when Safe Haven performed this work. *Id.* Approximately two months later, on August 16, 2017, Plaintiff filed a motion for preliminary injunction and a supporting memorandum of law requesting that Defendants return all confidential information held in escrow. Docs. 21, 22. In a letter dated August 28, 2017, Defendants' lawyer wrote that he had attempted to return the hard drive that contained the Law Firm's confidential information that he held in escrow on at least

four occasions between March 17, 2017, and August 28, 2017. Doc. 27. On August 28, 2017, Gorkic and Cullen affirmed that CAPEMS maintained Plaintiff's backup data on CAPEMS' server from January 2012 until the date of the affirmations and that "the entirety of Plaintiff's Confidential Information on Defendants' server has been forever deleted." Docs. 27-1, 27-2. Gorkic testified that no data was disturbed and that the methodology used to copy the backup was "forensically sound." Doc. 102-12, 23.

On August 31, 2017, Plaintiff represented to the Court that it had received a hard drive containing its confidential information and that it withdrew its motion for preliminary injunction. Doc. 28.

In a declaration submitted in opposition to the motion for summary judgment, Alexander Urbelis, an attorney with the Blackstone Law Group, a firm that also represents the Law Firm, stated that he provided the hard drive containing the Law Firm's backup that had been held in escrow to a data forensic consultant, Snowfensive LLC. Doc. 103. Urbelis then relates the results of the analysis of the hard drive conducted by Snowfensive, including that certain files appeared to be altered. *Id.*

On September 15, 2017, Plaintiff provided its Rule 26(a)(1) initial disclosures. Doc. 96-2. In those initial disclosures, Plaintiff stated that it was difficult to itemize its damages "because the damages are intangible," and that it would supplement the information as litigation progressed. *Id.* at 6–9.

On February 26, 2018, more than a year after the contractual relationship between Plaintiff and Defendants was terminated, and more than eight months after the filing of the instant suit, Safe Haven purchased a new firewall for the Law Firm. Doc. 102-28, 2. On March 9, 2018, a senior network technician installed the firewall, programmed it, and performed other

related tasks. Safe Haven charged the Law Firm $962.50 for the work related to the firewall's installation. Doc. 102-29, 2–4.

On July 31, 2018, all fact discovery ended and, two weeks later, on August 14, 2018, Plaintiff provided a more exact amount of damages. Doc. 96-3. Specifically, it claimed $6,000 for five years of monthly payments made despite Defendants' alleged breach, $199 for the purchase of a Windows 10 operating system, $5,000 for revenue lost as a result of Defendants' failures, $150 for a new hard drive, $900 for the diminished value of a Sony Tablet, $1,058.06 paid to Mumtaz's company to find "workarounds to Defendants' obstructive and spiteful behavior," $3,500 caused by email interruption, $11,103.75 to prosecute the preliminary injunction, and $6,000 for unspecified reasons. *Id.* at 4–8.

On October 22, 2018, the Law Firm filed yet a third statement of damages with its supplemental Rule 26(a)(1) initial disclosure. Doc. 102-5, 2. The Law Firm's new statement changed the total amount of damages claimed from $33,910.81 to $26,308.1. On the next day, October 23, 2018, the Law Firm filed a second amended Rule 26(a)(1) disclosure to correct a calculation error in the amount expended to prosecute the preliminary injunction. Doc. 102-6, 4.

During his deposition, Mohammedi provided the following explanation for the Law Firm's damages:

> Q. Sir, you're asking for monetary damages here?
> A. Right.
> Q. You say that you lost more than $5,000?
> A. I believe that's what's been lost. We are a very busy firm.
> Q. How do you calculate the $5,000?
> A. We are a very busy firm. That is actually in the Complaint. That is in the Complaint that is standard that we have put in.
> Q. I'm not asking about standard. It's a jurisdictional amount.
> A. Yes, but again, we lost money, we could not do the work. The firm could not do the work.

Q. This is the point where you get to say how you lost your money, how the firm lost more than $5,000 over the few days that you say you had no outbound and inbound e-mail service?

* * *

A. The money was lost because the lawyers could not do the work.[4]

Q. How much was lost?

A. It's put in there.

Q. No, no, no. This is a conclusion, more than 5,000. I need specifics.

A. We can provide you with specifics if you want.

Q. Please do. This is the time.

A. I'm not going to—I don't have that if front of me to provide specific amounts.

* * *

Q. You claim $5,000 in loss?

A. Approximately.

Q. For what period of time are we talking about?

A. I can't remember. It was a period of time that we could not have access to e-mails and the lawyers could not do the work, the paralegal could not do work, no one could do any work. . . The law firm, the lawyers could not do the work. They spend a lot of time back and forth, the disconnecting of the e-mails, could not do anything about this.

Q. Okay.

A. Rather than spending time on the cases, the firm was spending time trying to get the server back, the e-mails work properly and all this.

* * *

A. They could not send e-mails. It was disconnected. They could not do anything. I can't remember. At that time we had a lot of things going on. They shut everything on us.

Q. The e-mails. Outgoing e-mails were not working for a few days?

A. Yes. We relied on e-mails tremendously in our work.

* * *

Q. Tell us how your firm lost more than $5,000.

A. I explained this to you. That is enough. I explained how we lost money.

Doc. 96-5, 3–11.

[4] In an October 18, 2018 order, Magistrate Judge Pitman memorialized the Law Firm's stipulation that it would not offer any evidence of damages arising from two attorneys' inability to work or meet deadlines due to Defendants' alleged conduct. Doc. 86, 1–2.

II. Standard

Summary judgment is appropriate where "the movant shows that there is no genuine dispute as to any material fact." Fed. R. Civ. P. 56(a). "An issue of fact is 'genuine' if the evidence is such that a reasonable jury could return a verdict for the non-moving party." *Senno v. Elmsford Union Free Sch. Dist.*, 812 F.Supp.2d 454, 467 (S.D.N.Y. 2011) (citing *SCR Joint Venture L.P. v. Warshawsky*, 559 F.3d 133, 137 (2d Cir. 2009)). A fact is "material" if it "might affect the outcome of the suit under the governing law." *Id.* (internal quotation marks omitted). The party moving for summary judgment is first responsible for demonstrating the absence of any genuine issue of material fact. *Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986). If the moving party meets its burden, "the nonmoving party must come forward with admissible evidence sufficient to raise a genuine issue of fact for trial in order to avoid summary judgment." *Saenger v. Montefiore Med. Ctr.*, 706 F.Supp.2d 494, 504 (S.D.N.Y. 2010) (internal quotation marks omitted) (citing *Jaramillo v. Weyerhaeuser Co.*, 536 F.3d 140, 145 (2d Cir. 2008)). However, "When the burden of proof at trial would fall on the nonmoving party, it ordinarily is sufficient for the movant to point to a lack of evidence to go to the trier of fact on an essential element of the nonmovant's claim." *Jaramillo v. Weyerhaeuser Co.*, 536 F.3d 140, 145 (2d Cir. 2008).

III. Discussion

The Law Firm claims violations of the CFAA, breach of contract, breach of covenant of good faith and fair dealing, conversion, trespass to chattel, unjust enrichment, and tortious interference with a contract and business relationship.

For its claim under the CFAA, the Law Firm invokes the Court's federal question jurisdiction, pursuant to 28 U.S.C. § 1331. Doc. 12, 4. For its remaining state law claims, the Law Firm relies on the Court's supplemental jurisdiction, pursuant to 28 U.S.C. § 1367(a).

A. Computer Fraud Abuse Act

The Law Firm claims that Defendants violated the CFAA. The CFAA is a criminal statute, and it provides that "(a) [w]hoever . . . (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . (C) information from any protected computer . . . shall be punished." 18 U.S.C. § 1030 (a)(2)(c).

The CFAA also provides a civil cause of action for "[a]ny person who suffers damage or loss by reason of a violation of this section . . . only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i)." 18 U.S.C. § 1030(g). As relevant to this case, subclause (I) provides as follows: "Loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value." 18 U.S.C. § 1030 (c)(4)(A)(i)(I).[5]

The term "protected computer" means a computer "which is used in or affecting interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B). No party disputes that the Law Firm's computers qualified as protected computers. As a result, the resolution of this motion turns on whether Defendants accessed the Law Firm's computers without or in excess of authorization and whether, as a result of that unauthorized access, the Law Firm suffered a $5,000 loss "during any 1-year period."

[5] The parties agree that the remaining categories are not relevant here: "(II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals; (III) physical injury to any person; (IV) a threat to public health or safety; (V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security." 18 U.S.C. § 1030 (c)(4)(A)(i).

1. Damages[6]

To maintain a cause of action under the CFAA against a defendant, a plaintiff must demonstrate that the defendant violated the CFAA in "*a manner that has caused* [the plaintiff] damages or losses of at least $5,000." *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 440 (2d Cir. 2004) (emphasis added).

"A number of courts in this district have held that losses under the CFAA are compensable only when they result from damage to, or the inoperability of, the accessed computer system." *New London Assocs., LLC v. Kinetic Soc. LLC*, No. 18 Civ. 7963 (DLC), 2019 WL 1570809, at *9 (S.D.N.Y. Apr. 11, 2019) (citing *Civic Center Motors, Ltd. v. Mason Street Import Cars, Ltd.*, 387 F. Supp. 2d 378, 381 (S.D.N.Y. 2005); *Massre v. Bibiyan*, No. 12 Civ. 6615 (KPF), 2014 WL 2722849 at *3 (S.D.N.Y. June 16, 2014); *Poller v. BioScrip*, 974 F. Supp. 2d 204, 232 (S.D.N.Y. 2013); *Nexans Wires S.A. v. Sark-USA, Inc.*, 319 F. Supp. 2d 468, 474 (S.D.N.Y. 2004)).[7] According to the statute's own definition, "the term 'damage' means any impairment to the integrity or availability of data, a program, a system, or information . . . ." 18 U.S.C. § 1030(e)(8).

As a result, "[c]ourts in the Southern District of New York have interpreted 'loss' narrowly, rejecting arguments, for example, that it includes the economic value of consumers'

---

[6] To be sure, a court does not typically address the issue of damages unless it has determined that liability exists. Here, however, Defendants expend almost the entirety of their argument asserting that Plaintiff has not established damages. Accordingly, the Court will address the issue of damages first.

[7] *See also Univ. Sports Pub. Co. v. Playmakers Media Co.*, 725 F. Supp. 2d 378, 388 (S.D.N.Y. 2010) (because "the audit sought to identify ways to improve the database's security systems, not to identify and address damage caused by the security breach that had already taken place," the cost "probably does not fall within the statutory definition of 'loss.'"); *Tyco Int'l (US) Inc. v. John Does, 1-3*, No. 01 Civ. 3856 (RCC)(DF), 2003 WL 23374767, at *3 (S.D.N.Y. Aug. 29, 2003) ("the additional types of damages awarded by courts under the Act have generally been limited to those costs necessary to assess the damage caused to the plaintiff's computer system or to resecure the system in the wake of a spamming attack.").

attention, that it includes the cost of business trips undertaken to respond to a computer hacking incident, or that it includes lost profits that are not attributable to an 'interruption of service.'" *B.U.S.A. Corp. v. Ecogloves, Inc.*, No. 05 Civ. 9988 (JSR), 2009 WL 3076042, at *6 (S.D.N.Y. Sept. 28, 2009) (citing *In re Doubleclick Inc. Privacy Litigation,* 154 F.Supp.2d 497, 524–25 (S.D.N.Y.2001) and *Nexans Wires S.A. v. Sark–USA, Inc.,* 319 F.Supp.2d 468, 473–76 (S.D.N.Y.2004), *aff'd by summary order,* 166 Fed. Appx. 559 (2d Cir.2006)). *See also Garland-Sash v. Lewis*, No. 05 CIV 6827 WHP, 2011 WL 6188712, at *3 (S.D.N.Y. Dec. 6, 2011) ("CFAA defines these terms narrowly.").

Along the same lines, courts within this District have dismissed CFAA claims for failing to sufficiently quantify damages. *See Bose v. Interclick, Inc.*, No. 10 Civ. 9183 DAB, 2011 WL 4343517, at *4 (S.D.N.Y. Aug. 17, 2011) (finding that Plaintiff's "claims therefore fail because she does not quantify the repair cost or cost associated with investigating the alleged damage."); *Fink v. Time Warner Cable*, No. 08 Civ. 9628 LTS KNF, 2009 WL 2207920, at *4 (S.D.N.Y. July 23, 2009) (finding that the "Plaintiff has failed to plead adequately her claim for a violation of the CFAA" because she merely alleged that "Defendant causes damage by impairing the integrity or availability of data and information, as well as certain communications and protocols.").

The Law Firm claims that it satisfied the loss requirement because it paid Safe Haven $1,058.06 for resolving problems with the Law Firm's wireless network and printing in January 2017, $2,828.99 for a new backup system in June 2017, $703 for a new firewall on February 26, 2018, and $962.50 for its installation on March 9, 2018. Doc. 101, 13. These damages add up to $5,552.55.

None of the evidence proffered by the Law Firm establishes a causal relationship between the alleged unauthorized access and the damages alleged. Doc. 101, 15–16. Mohammedi and Mumtaz

testified that the Law Firm paid these invoices because CAPEMS terminated the contract[8] and because CAPEMS provided inadequate service,[9] but they did not establish, according to the records provided to the Court, that the Law Firm suffered these damages because CAPEMS accessed the Law Firm's computers without authorization. In other words, the costs incurred by the Law Firm involve efforts to enhance its systems and address inadequate services by CAPEMS during the period that CAPEMS had authority to access the system. The costs described in the invoices simply reflect either negligence on the part of Defendants or the costs inherent in changing computer system contractors, including creating systems to ensure that the prior contractor cannot access the system.[10] Even assuming, arguendo, that Defendants provided inadequate service, such inadequacy may state a claim for breach of contract, but it does not state a CFAA violation. Because the Law Firm has failed to produce any evidence that it suffered damages compensable by the CFAA, Plaintiff's CFAA claim may be dismissed on this ground.

Moreover, even if the Law Firm had established that these damages were the result of Defendants' unauthorized access, its CFAA claim would still fail because the Law Firm could not aggregate the losses for the purposes of satisfying the $5,000 loss requirement. Indeed, the

---

[8] When asked specifically to identify the Law Firm's damages, Mohammedi claimed that the Law Firm suffered damages because the Law Firm "ha[d] to spend quite a lot of money to get this backup set." Doc. 102-11, 28.

[9] Mohammedi testified about creating a backup "the way it should be done," installing a secure server, and stabilizing the network after the contract's termination. Doc. 102-11, 29–30, 53, 56–57, 73–74. Along the same lines, Mumtaz testified that he discovered "weak passwords," no backup, and an "insecure VPN due to the work CAPEMS did." Doc. 102-10, 14–16.

[10] In opposition to the motion for summary judgment, Mumtaz affirmed that "[t]he work done by Safe Haven was absolutely required in order to restore the server and correct Defendants' breach." Doc. 104, 8. However, Mumtaz previously testified in his deposition that the reason that he recommended replacing the server was because he did not "like" the older one and because the newer one was "new, faster, better, shinier." Doc. 96-12, 4. He also testified that he reviewed the Law Firm's network and server because "it's a common practice." 102-10, 14–16. As a result, the affidavit alleging unauthorized access does not preclude summary judgment because "a party may not create an issue of fact by submitting an affidavit in opposition to a summary judgment motion that, by omission or addition, contradicts the affiant's previous deposition testimony." *Hayes v. New York City Dep't of Corr.*, 84 F.3d 614, 619 (2d Cir. 1996).

statute requires "loss to 1 or more persons during *any 1-year period* . . . aggregating at least $5,000 in value," 18 U.S.C. § 1030 (c)(4)(A)(i)(I) (emphasis added), and the loss alleged here occurred over a period of at least fourteen months, from January 2017 to March 2018. By Plaintiff's own reckoning, the costs were incurred as follows:

- January 2017, $1,058.06
- June 2017, $2,828.99
- February 2018, $703
- March 2018, $962.50
- Total: $5,552.55

Doc. 101, 13. Given these representations, it is impossible for Plaintiff to establish the requisite loss within one year. Indeed, if the Court considered the twelve-month period beginning in January 2017, the loss amount would only total $3,887.05, and if the Court measured the twelve-month period ending in March 2018, the loss amount would only equal $4,494.49. As a result, this provides another reason for finding that the Law Firm has not satisfied the CFAA's loss requirement. [11]

---

[11] Even if the Law Firm had suffered the requisite damages in a one-year period, it is unclear whether it would be able to establish that Defendants accessed its computers without authorization. A person may violate the CFAA either by "access[ing] a computer without authorization or exceeding authorized access." 18 U.S.C. § 1030(a)(1). According to the statutory definition, "'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter . . ." 18 U.S.C. § 1030(e)(6). In summarizing the statute's legislative history, the Second Circuit found that it "characterizes the evil to be remedied—computer crime—as 'trespass' into computer systems or data, and correspondingly describes 'authorization' in terms of the portion of the computer's data to which one's access rights extend." *United States v. Valle*, 807 F.3d 508, 525 (2d Cir. 2015).

A number of courts within this District have held that a civil CFAA case will not succeed unless the plaintiff shows "that [d]efendants accessed its computer system without approval." *Chefs Diet Acquisition Corp. v. Lean Chefs, LLC*, No. 14 Civ. 8467 (JMF), 2016 WL 5416498, at *6 (S.D.N.Y. Sept. 28, 2016). Furthermore, the cases explain that "the statute does not apply to a 'so-called faithless or disloyal employee' — that is, an employee who has been granted access to an employer's computer and misuses that access." *Chefs Diet Acquisition Corp. v. Lean Chefs*, LLC, No. 14 Civ. 8467 (JMF), 2016 WL 5416498, at *6 (S.D.N.Y. Sept. 28, 2016). *See also Apple Mortg. Corp. v. Barenblatt*, 162 F. Supp. 3d 270, 286 (S.D.N.Y. 2016) ("If an employer has given an employee

B. State Law Claims

Under 28 U.S.C. § 1367(c)(3), the Court may decline to exercise jurisdiction over any non-federal claims over which it could have supplemental jurisdiction if the Court has dismissed all of the claims over which it has original jurisdiction. Subject matter jurisdiction in the instant action is based on federal question, 28 U.S.C. § 1331. The Court "may decline to exercise supplemental jurisdiction over" state claims if: "(1) the claim raises a novel or complex issue of State law, (2) the claim substantially predominates over the claim or claims over which the district court has original jurisdiction, (3) the district court has dismissed all claims over which it

---

access to the computer and to the relevant files, the employee's subsequent misuse of the information or misappropriation with the intent to compete with his employer is not sufficient to violate the CFAA.").

For this reason, Defendants argue that they did not access the Law Firm's computer without authorization. Doc. 96, 12. During their contract with the Law Firm, and in accordance with the contract, they installed applications on the Law Firm's computers to send information automatically to their servers to backup the Law Firm's information remotely. Doc. 102-15, 27–30. After the termination of their contract with the Law Firm, Defendants emailed Mumtaz to explain that they had previously installed this software, that they continued to receive information from the Law Firm's computers, and that the Law Firm "probably should uninstall any remaining items we had installed," related to monitoring. *Id.*

In attempting to create a genuine issue of material fact on whether Defendants accessed the Law Firm's computers without authorization, Plaintiff focuses on Mumtaz's affidavit, submitted in opposition to the motion for summary judgment. Doc. 101, 17. In it, Mumtaz affirms that neither he, nor anyone at Safe Haven, had given authorization for Defendants to access the network. Doc. 104, 6. This testimony, however, is irrelevant because the question is whether the Law Firm—not Safe Haven—authorized Defendants to install the remote backup applications on the Law Firm's computers. And more to the point, the contract between the Law Firm and Defendants establishes that authorization had, in fact, been given; Defendants installed software that allowed them to remotely backup the Firm's files, and the new contractor was specifically advised to uninstall the software. Thus, whatever access Defendants continued to have was with "authorization."

Next, it alleges that, in Gorkic's deposition, he explained his decision to notify Mumtaz about the automatic backup on the Law Firm's computers, and his unwillingness to delete the applications from the Law Firm's computer himself because he feared being accused of accessing the Law Firm's computers without authorization. Doc. 102-12, 14, 18. That testimony merely reinforces Defendants' assertion that they installed the applications on the Law Firm's computers pursuant to the Law Firm's request.

Finally, the Law Firm's reliance on Urbelis's declaration is unavailing. As Urbelis makes clear, the substance of the declaration is a recitation of the analysis conducted by a third person at Snowfensive, and is accordingly inadmissible rank hearsay. Fed. R. Civ. P. 56(c)(4) ("An affidavit or declaration used to support or oppose a motion must be made on personal knowledge, set out facts that would be admissible in evidence, and show that the affiant or declarant is competent to testify on the matters stated.").

has original jurisdiction, or (4) in exceptional circumstances, there are other compelling reasons for declining jurisdiction." 28 U.S.C. § 1367(c).

Having disposed of the Law Firm's only federal claim, it would be inappropriate to adjudicate its state law claims. Therefore, the Court declines to retain jurisdiction over the state law claims and dismisses them without prejudice. *See United Mine Workers v. Gibbs,* 383 U.S. 715, 726 (1966) (stating that, if the federal claims are disposed of before trial, "the state claims should be dismissed as well.").

IV. Conclusion

For the foregoing reasons, Defendants' Motion for Summary Judgment on the federal claim is GRANTED. This Court declines to retain supplemental jurisdiction over the state law claims against them and therefore those claims are DISMISSED without prejudice. The Clerk of the Court is respectfully directed to terminate this motion, Doc. 94, and close the case.

It is SO ORDERED.

Dated: July 22, 2019
New York, New York

Edgardo Ramos, U.S.D.J.